(19)Title

A Proposal to identify unsafe control actions in STAMP/STPA by simulation using State Transition Specification of Control Structure and guide word

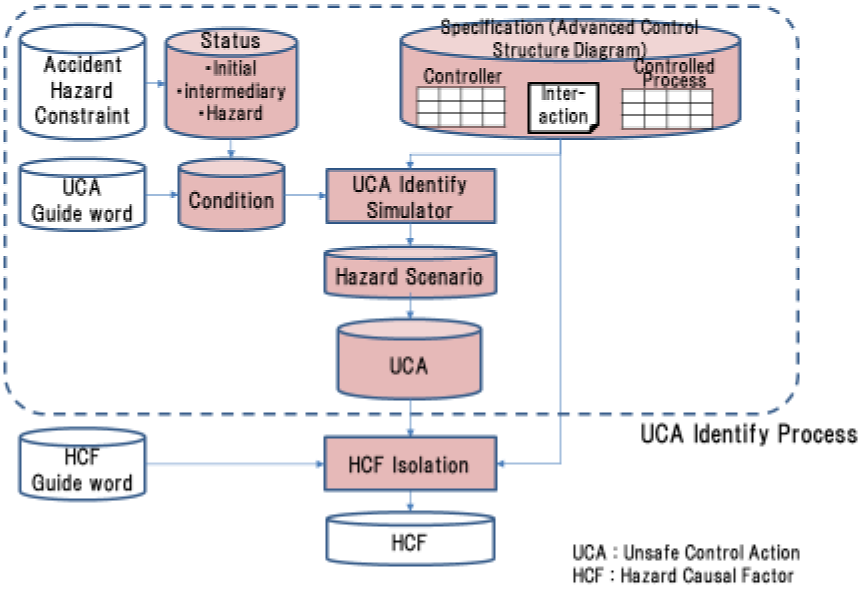
Speaker, Authors

Osaka Institute of Technology. Yasuko FUKUZAWA

Abstract

“STAMP/STPA” is useful method for safety and security analysis of complicated system such as Internet of Things and Cyber-Physical System. By using this method, software abnormality and interaction abnormality between components on system are identified. This method consists of two steps. [Step 1] Identify unsafe control actions (UCA) leading to a hazard in accordance with a guide word from a control structure showing an intersystem configuration. [Step 2] Identify a hazard causal factor for each UCA according to a guide word. It is difficult to analyze cyclopaedically with the guide word. So to reduce the analysist's load of UCA identification, we propose the following method to identify UCA leading to hazards by using state transition specification and simulation. The specifications of the controller and controlled target in the control structure are represented by state transition tables. Then the UCA is identified by simulating the reachability to the hazard state on the state transition tables according to the guide word for CA. We report the effectiveness and approach of the method to identify UCA using state transition tables and simulation.

UCA semi-automatic identification method using state transition table



Keywords

(1) system safety (security) analysis

(2) STAMP/STPA

(3) finite state machine

(4) state transition table

(5) reachability analysis